

# Random multiparty entanglement distillation

Ben Fortescue\* and Hoi-Kwong Lo†

*Center for Quantum Information and Quantum Control (CQIQC),  
Dept. of Electrical & Computer Engineering and Dept. of Physics,  
University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

(Dated: January 15, 2008)

We describe various results related to the random distillation of multiparty entangled states - that is, conversion of such states into entangled states shared between fewer parties, where those parties are not predetermined. In previous work [1] we showed that certain output states (namely Einstein-Podolsky-Rosen (EPR) pairs) could be reliably acquired from a prescribed initial multipartite state (namely the  $W$  state  $|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$ ) via random distillation that could not be reliably created between predetermined parties. Here we provide a more rigorous definition of what constitutes “advantageous” random distillation. We show that random distillation is always advantageous for  $W$ -class three-qubit states (but only sometimes for Greenberger-Horne-Zeilinger (GHZ)-class states). We show that the general class of multiparty states known as symmetric Dicke states can be readily converted to many other states in the class via random distillation. Finally we show that random distillation is provably not advantageous in the limit of multiple copies of pure states.

## I. INTRODUCTION

Entanglement in quantum information theory is often considered as a resource [2, 3] which can be used by physically separated parties to perform tasks such as quantum teleportation [4] or superdense coding [5], under the restriction of the parties to local operations and classical communications (LOCC). Under LOCC the parties can perform local quantum operations on their own portions of the entangled states and exchange classical information with each other through some classical communication channels, but not perform joint quantum operations or (equivalently) exchange quantum information. It is known that parties cannot increase their shared entanglement under LOCC, which motivates the view of entanglement as a resource.

Determining what may be accomplished with some particular entangled state under LOCC provides an operational description of that state, which can in some cases be used as an entanglement measure - for example the well-known result [6] that the maximum ratio at which maximally-entangled EPR pairs

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \quad (1)$$

can be obtained through LOCC is the entanglement entropy  $E^S(\psi_{AB}) = S(\rho_A)$ , where

$$S(\rho) = -\text{tr} \rho \log_2 \rho \quad (2)$$

$$\rho_A = -\text{tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|). \quad (3)$$

In general, the properties of multiparty entangled states (those shared between more than two parties) are

much less-well understood than those of two-party states. For example, there is no single well-defined maximally entangled state in the multiparty case. It appears that multiparty states can be divided into distinct classes [7, 8], and even in the three-party case it is not known whether or not all entangled states can be reversibly obtained through LOCC from a finite selection of other states - the “minimal reversible entanglement generating set” (MREGS) [9].

A topic of interest in the description of multiparty entangled states is the conversion of these states into, generally, states shared between fewer parties, and specifically two-party states. Since there are many results on the operational properties of two-party states, considering such a conversion provides useful information in the multiparty case.

Several results e.g. [10, 11, 12, 13, 14, 15] exist regarding the conversion of multiparty to two-party entangled states shared between predetermined parties. In [1] we demonstrated that some two-party entangled states which could not be reliably obtained (i.e. probability  $< 1$ ) between predetermined parties could be reliably obtained (probability  $\rightarrow 1$  in the limit of many “rounds” of distillation) between parties which were randomly determined in the course of a LOCC-protocol - a process we refer to as “random distillation”. Specifically we showed that one can reliably distill one EPR pair from a single  $W$  between random parties, versus doing so with a probability at most  $2/3$  between predetermined parties. The random distillation rate exceeds even the asymptotic rate of  $H_2(1/3) \approx 0.92$  EPRs per  $W$  between predetermined parties in the many-copy limit, where  $H_2$  is the binary entropy function

$$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x). \quad (4)$$

In this paper, we address a number of questions in random distillation. Firstly, our criterion in [1] for what constituted “advantageous” random distillation was some-

\*bfort@physics.utoronto.ca

†hklo@comm.utoronto.ca

what problematic, in particular when considering multiple copies of states. Here we provide a new criterion for advantageous random distillation applicable to any pure-state case, including that of collective operations on multiple copies of a state. We also ask whether random distillation gives an advantage in the many-copy limit, and demonstrate that it does not.

Secondly, in our previous paper we considered only a small number of specific states. Here we consider the random distillation properties of general classes of states - specifically, distilling the general classes of three-qubit pure-state entanglement, the GHZ and  $W$  classes. We show that all  $W$ -class states can undergo advantageous random distillation, but the GHZ class contains examples both of states which can and cannot.

Finally, we previously considered primarily distillation to two-party EPR pairs. Here we consider a class of final states shared between larger numbers of parties. For the multiparty entangled states known as symmetric Dicke states, we briefly demonstrate a class of output states which may be reliably obtained through LOCC only by random distillation.

## II. DEFINITIONS

For conversion of an  $M$ -party pure state  $|\psi\rangle$  to EPR pairs  $|\Phi\rangle$  through LOCC

$$|\psi\rangle_{A_1 \dots A_M}^{\otimes N} \xrightarrow[\text{LOCC}]{ij} \bigotimes_{ij} |\Phi\rangle_{A_i A_j}^{\otimes N_{A_i A_j}}. \quad (5)$$

we define

$$E_{a_{IJ}}^\infty(\psi) \equiv \sup_{N \rightarrow \infty} \frac{N_{A_I A_J}}{N} \quad (6)$$

$$E_s^\infty(\psi) \equiv \max_{ij} \sup_{N \rightarrow \infty} \frac{N_{A_i A_j}}{N} \quad (7)$$

$$E_t^\infty(\psi) \equiv \sup_{N \rightarrow \infty} \frac{\sum_{ij} N_{A_i A_j}}{N}. \quad (8)$$

That is,  $E_{a_{IJ}}^\infty$  represents the maximum rate of EPR distillation between parties  $I$  and  $J$  (with the help of all other parties),  $E_s^\infty$  represents the highest distillation rate of EPR pairs between any given pair of parties and  $E_t^\infty$  the highest total EPR distillation rate, irrespective of which parties share them.

In this asymptotic case (though not generally)  $E_{a_{IJ}}^\infty$  is equal to the entanglement of assistance [10], with [13] showing that

$$E_{a_{IJ}}^\infty = \min_T \{S(\rho_{A_I T}), S(\rho_{A_J \bar{T}})\} \quad (9)$$

where the minimization is over the division of parties other than  $A_I$  and  $A_J$  into two groups  $T$  and  $\bar{T}$  (i.e. over bipartite “cuts” separating all parties into two groups, one containing  $A_I$  and one containing  $A_J$ ) and

$$\rho_{A_I T} = \text{tr}_{A_j \notin \{I, T\}} (|\psi\rangle\langle\psi|), \quad (10)$$

the reduced state of  $|\psi\rangle\langle\psi|$ , traced over all  $A_j \notin \{I, T\}$ .

For the single-copy analogues of these quantities, for the distillation

$$|\psi\rangle_{A_1 \dots A_M} \xrightarrow[\text{LOCC}]{ij} \bigotimes_{ij} |\Phi\rangle_{A_i A_j}^{\otimes N_{A_i A_j}}, \quad (11)$$

we define

$$E_{a_{IJ}}(\psi) \equiv \sup \langle N_{A_I A_J} \rangle \quad (12)$$

$$E_s(\psi) \equiv \max_{ij} (\sup \langle N_{A_i A_j} \rangle) \quad (13)$$

$$E_t(\psi) \equiv \sup \left\langle \sum_{ij} N_{A_i A_j} \right\rangle \quad (14)$$

We noted in [1] that for the three-party  $W$  state

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{ABC} \quad (15)$$

it is possible to obtain an EPR through LOCC between random parties but not specified parties. Hence even though (from [13])  $E_s^\infty(W) = H_2(1/3) \approx 0.92$ , we find  $E_t^\infty(W) \geq 1$ . However [1] further noted that the condition  $E_t > E_s$  could also be trivially satisfied, for example by the state  $|\Phi\rangle_{AB} \otimes |\Phi\rangle_{BC}$ , for which  $E_t = 2 > E_s = 1$ .

We would therefore like to find a condition that more generally captures when true “random distillation” is advantageous - that is, one obtains a greater entanglement yield due to the nondeterministic nature (in terms of which parties receive the final state) of the distillation, rather than there simply being somewhat independent entanglements between different pairs of parties. We would further like to define such a condition in terms of general pure-state bipartite entanglement measures, rather than solely in terms of the distillable EPR pairs.

We thus consider the LOCC-conversion (via a protocol  $P$ ) of an initial pure state  $\psi$  to final pure multipartite states  $\psi_f$  with probabilities  $p_f$ .

$$\psi \xrightarrow[\text{LOCC}]{P} \{\psi_f, p_f\} \quad (16)$$

and the LOCC conversion (via a protocol  $Q$ ) of multi-party states  $\psi_f$  to pure two-party states  $\psi_{gIJ}$  with probabilities  $p_g$

$$\psi_f \xrightarrow[\text{LOCC}]{Q} \{\psi_{gIJ} \otimes \rho_g, p_g\} \quad (17)$$

(note that in the above,  $I$  and  $J$  are not necessarily the same for every  $g$ ).

We define, for some bipartite pure-state entanglement

measure  $E$

$$A_{IJ}(\psi_f) \equiv \sup_{P,Q} \sum_g p_g E(\psi_{gIJ}) \quad (18)$$

$$E_{sp}(\psi_f) \equiv \max_{IJ} A_{IJ}(\psi_f) \quad (19)$$

$$E_{rnd}(\psi) \equiv \sup_{P,Q} \sum_f p_f E_{sp}(\psi_f) \quad (20)$$

$$E_{rnd}^\infty(\psi) \equiv \frac{E_{rnd}(\psi^{\otimes N})}{N}, \quad N \rightarrow \infty \quad (21)$$

$$E_{sp}^\infty(\psi) \equiv \frac{E_{sp}(\psi^{\otimes N})}{N}, \quad N \rightarrow \infty \quad (22)$$

where the supremums in the above expressions are over all possible LOCC protocols  $P$  and  $Q$ .

Hence  $E_{rnd}$  represents the supremum of the expected entanglement (as measured by  $E$ ) obtained by whichever pair of parties has the highest entanglement once the protocol has been performed, while  $E_{sp}$  is the corresponding quantity for parties chosen before performing the protocol. Thus  $E_{rnd} \geq E_{sp}$  in general, and, if  $E_{rnd}(\psi) > E_{sp}(\psi)$ , this represents genuine advantageous random distillation as discussed above.

While as mentioned any bipartite pure-state measure  $E$  may in principle be used, for the remainder of this paper and our results (with the exception of Section IV) we shall adopt as our measure the entanglement entropy  $E^S$ , i.e. the Von Neumann entropy  $S$  of the reduced state as noted above. We thus define

$$E(\psi_{AB}) \equiv E^S(\psi_{AB}). \quad (23)$$

### III. W AND GHZ-CLASS STATES

In [1] we demonstrated advantageous random distillation for the three-party  $W$  and similar states, and that random distillation was not advantageous for certain GHZ-like states. However no general result was obtained for the general GHZ and  $W$  classes noted in [7], into one of which any three-qubit pure state with genuine tripartite entanglement may be classed. Here we find

#### Theorem 1:

For any  $W$ -class pure entangled three-qubit state  $\psi_W$

$$E_{rnd}(\psi_W) > E_s(\psi_W) \quad (24)$$

#### Proof:

We make use of the following simple lemma

**Lemma 1:** For a general normalised two-qubit pure state

$$\psi = (c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle)_{AB} \quad (25)$$

the entanglement measure  $S(\rho_A)$  increases monotonically with the concurrence [16]

$$q(\psi) = 2|c_{01}c_{10} - c_{00}c_{11}| \quad (26)$$

and  $S(\rho_A)$  is a convex function of  $q(\psi)$  in the range  $0 \leq q \leq 1$ , corresponding to  $0 \leq S \leq 1$ .

**Proof:** Explicit calculation shows

$$S(\rho_A) = f(q) = H_2\left(\frac{1 - \sqrt{1 - q(\psi)^2}}{2}\right) \quad (27)$$

and that

$$\frac{d^2 f}{dq^2} \geq 0, \quad 0 \leq S \leq 1 \quad \square \quad (28)$$

We define  $q_{sp}$ ,  $q_{rnd}$  etc. as analogous quantities to  $E_{sp}$ ,  $E_{rnd}$  etc., with  $q$  as the entanglement measure. The quantity  $q$  is a useful measure in this case since it is second-order in the state's coefficients. Thus, for repeated rounds of unitaries and measurements, probabilities and normalisation factors cancel out when calculating  $\langle q \rangle$ , as shown below. Since the  $E_x$  (i.e.  $E_{rnd}$ ,  $E_{sp}$  etc.) are expectation values for  $S$ , it follows from the convexity result that

$$E_x(\psi) \geq f(q_x(\psi)). \quad (29)$$

Note then that by this definition  $q_x(\psi) \neq f^{-1}(E_x(\psi))$ , in general.

#### A. The $W$ protocol

We first consider the protocol of [1] (which we will refer to as the  $W$  protocol) for obtaining an EPR pair from a  $W$  state. This consists of all three parties repeatedly applying the unitary

$$|0\rangle \longrightarrow \sqrt{1 - \epsilon^2}|0\rangle + \epsilon|2\rangle, \quad |1\rangle \longrightarrow |1\rangle \quad (30)$$

followed by all performing the projection

$$F = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad G = |2\rangle\langle 2|. \quad (31)$$

If all three parties get outcome  $F$ , the protocol is repeated. If exactly one party gets outcome  $G$ , the other two parties have an EPR pair, the expectation value of their eventual entanglement tending to unity in the limit of many repetitions and small  $\epsilon$ . (The probability of the protocol aborting due to failure, where two or more parties get  $G$ , is negligible in this limit).

(We also show in [1] that random distillation is advantageous for a finite number of rounds, with a protocol for which the probability of obtaining a randomly-shared EPR pair from a  $W$  within  $R$  rounds is  $\frac{R}{R+1}$ . This exceeds the single-copy limit (for predetermined parties) of  $2/3$  for  $R \geq 3$  and the asymptotic limit of  $0.92$  for  $R \geq 12$ .)

Note that the  $W$  state enjoys a special property that makes our previous analysis of random distillation of an EPR from a  $W$  state simple - a failed round (that is,

where all parties obtain outcome  $F$ ) returns the state to a  $W$ . Therefore in the limit of many rounds and small  $\epsilon$  (where success and failure of this kind are the only outcomes with non-negligible probability) the protocol is “reset” after each failure and every round can be analysed in the same way. In contrast, this is *not* the case for a general three-qubit pure state. Indeed, whenever a round of random distillation fails a general three-qubit state becomes a new state. For this reason, the analysis of multi-round random distillation for the general three-qubit state is not entirely trivial. In the following, we will use the properties of the concurrence discussed above to perform such an analysis. Before doing so, let us first demonstrate the evolution of a general three-qubit state under the  $W$  protocol.

Consider then applying this protocol to a general three-qubit pure state shared between Alice, Bob and Charlie:

$$|\psi_1\rangle_{ABC} = |0\rangle_A \left( k_{00_0}|00\rangle + k_{01_0}|01\rangle + k_{10_0}|10\rangle + k_{11_0}|11\rangle \right)_{BC} + |1\rangle_A(\dots) \quad (32)$$

where the (...) represent some additional terms whose amplitudes we are not concerned with. We define  $K_{00_0} \equiv |k_{00_0}|^2$  etc.

After every party has performed the unitary (30) the state becomes

$$\begin{aligned} |\psi_1\rangle_{ABC} = & (1 - \epsilon^2)^{\frac{1}{2}} |0\rangle_A \left( (1 - \epsilon^2)k_{00_0}|00\rangle \right. \\ & \left. + (1 - \epsilon^2)^{\frac{1}{2}}[k_{01_0}|01\rangle + k_{10_0}|10\rangle] + k_{11_0}|11\rangle \right)_{BC} \\ & + \epsilon |2\rangle_A \left( (1 - \epsilon^2)k_{00_0}|00\rangle + (1 - \epsilon^2)^{\frac{1}{2}}[k_{01_0}|01\rangle + k_{10_0}|10\rangle] \right. \\ & \left. + k_{11_0}|11\rangle \right)_{BC} + (\dots). \quad (33) \end{aligned}$$

If all the parties then perform the projection (31) and all get outcome  $F$  the resultant state will differ from the initial state. Likewise if these unitaries and projections repeat until Alice, say, eventually gets outcome  $G$  the state then shared by Bob and Charlie will depend on the number of rounds performed up to that point.

In general after  $R$  rounds of unitaries and projections in which all parties get  $F$ , the shared state will be

$$|\psi_R\rangle_{ABC} = |0\rangle_A \left( k_{00_R}|00\rangle + k_{01_R}|01\rangle + k_{10_R}|10\rangle + k_{11_R}|11\rangle \right)_{BC} + |1\rangle_A(\dots)_{BC} \quad (34)$$

where

$$k_{00_R} = \frac{(1 - \epsilon^2)^{\frac{3R}{2}} k_{00_0}}{\sqrt{P_{F_R} \dots P_{F_1}}} \quad (35)$$

$$k_{01_R} = \frac{(1 - \epsilon^2)^R k_{01_0}}{\sqrt{P_{F_R} \dots P_{F_1}}} \quad (36)$$

$$k_{10_R} = \frac{(1 - \epsilon^2)^R k_{10_0}}{\sqrt{P_{F_R} \dots P_{F_1}}} \quad (37)$$

$$k_{11_R} = \frac{(1 - \epsilon^2)^{\frac{R}{2}} k_{11_0}}{\sqrt{P_{F_R} \dots P_{F_1}}} \quad (38)$$

and  $P_{F_N}$  is the probability of all parties getting  $F$  in the  $N$ th round of the protocol after having done so in all previous rounds i.e.

$$\begin{aligned} P_{F_N} = & (1 - \epsilon^2) \left( (1 - \epsilon^2)^2 K_{00_{N-1}} \right. \\ & \left. + (1 - \epsilon^2)[K_{01_{N-1}} + K_{10_{N-1}}] + K_{11_{N-1}} \right) \quad (39) \end{aligned}$$

If the parties perform one further round of unitaries, the state will be

$$\begin{aligned} |\psi_{R+1}\rangle_{ABC} = & (1 - \epsilon^2)^{\frac{1}{2}} |0\rangle_A \left( (1 - \epsilon^2)k_{00_R}|00\rangle \right. \\ & \left. + (1 - \epsilon^2)^{\frac{1}{2}}[k_{01_R}|01\rangle + k_{10_R}|10\rangle] + k_{11_R}|11\rangle \right)_{BC} \\ & + \epsilon |2\rangle_A \left( (1 - \epsilon^2)k_{00_R}|00\rangle \right. \\ & \left. + (1 - \epsilon^2)^{\frac{1}{2}}[k_{01_R}|01\rangle + k_{10_R}|10\rangle] + k_{11_R}|11\rangle \right)_{BC} \\ & + (\dots) \quad (40) \end{aligned}$$

If the parties then project and Alice alone gets outcome  $G$ , with probability

$$P_{G_{R+1}} = \epsilon^2 \left( (1 - \epsilon^2)^2 K_{00_R} + (1 - \epsilon^2)[K_{01_R} + K_{10_R}] + K_{11_R} \right) \quad (41)$$

the resultant state will be

$$\begin{aligned} & \frac{1}{\sqrt{P_{G_{R+1}}}} \epsilon |2\rangle_A \left( (1 - \epsilon^2)k_{00_R}|00\rangle \right. \\ & \left. + (1 - \epsilon^2)^{\frac{1}{2}}[k_{01_R}|01\rangle + k_{10_R}|10\rangle] + k_{11_R}|11\rangle \right)_{BC} \quad (42) \end{aligned}$$

and Bob and Charlie will share a state with entanglement (measured by the concurrence  $q$  (26))

$$\begin{aligned} q_{R+1}^{BC} = & \frac{1}{P_{G_{R+1}}} \epsilon^2 (1 - \epsilon^2) \times 2 |k_{01_R} k_{10_R} - k_{00_R} k_{11_R}| \quad (43) \\ = & \frac{2}{P_{G_{R+1}} P_{F_R} \dots P_{F_1}} \epsilon^2 (1 - \epsilon^2)^{2R+1} \\ & \times |k_{01_0} k_{10_0} - k_{00_0} k_{11_0}| \quad (44) \end{aligned}$$

Thus if we consider applying the  $W$  protocol to an arbitrary three-qubit state we have that for the final expected concurrence  $\langle q_f^{BC} \rangle$  (26):

$$\langle q_f^{BC} \rangle \geq \lim_{\epsilon \rightarrow 0} \sum_{R=0}^{\infty} q_{R+1}^{BC} P_{G_{R+1}} \prod_{N=1}^R P_{F_N} \quad (45)$$

$$= 2|k_{01_0}k_{10_0} - k_{00_0}k_{11_0}| \times \lim_{\epsilon \rightarrow 0} \sum_{R=0}^{\infty} \epsilon^2 (1 - \epsilon^2)^{2R+1} \quad (46)$$

$$= 2|k_{01_0}k_{10_0} - k_{00_0}k_{11_0}| \times \lim_{\epsilon \rightarrow 0} \frac{\epsilon^2 (1 - \epsilon^2)}{1 - (1 - \epsilon^2)^2} \quad (47)$$

$$= |k_{01_0}k_{10_0} - k_{00_0}k_{11_0}|. \quad (48)$$

The above bound concerns only Bob and Charlie's entanglement as a result of Alice eventually getting outcome  $G$  (and the others  $F$ ). However other possible outcomes are where instead Bob or Charlie gets  $G$  resulting in zero Bob-Charlie entanglement, but some entanglement between Alice-Bob or Alice-Charlie. How much entanglement depends on the form of the original state, but since the  $W$  protocol is symmetric (i.e. invariant with respect to permutation of parties), we see that in the special case of a symmetric state  $\psi_{ABC}^{symm}$ , the expected entanglement due to such outcomes must also be  $|k_{01_0}k_{10_0} - k_{00_0}k_{11_0}| = |k_{01_0}^2 - k_{00_0}k_{11_0}|$  (since  $k_{01_0} = k_{10_0}$  for symmetric  $\psi_{ABC}$ ), for each of Alice-Bob and Alice-Charlie.

Thus, considering only these outcomes where two parties share some entanglement and are unentangled with the third party, it follows that

$$E_{rnd}(\psi_{ABC}^{symm}) \geq 3|k_{01_0}^2 - k_{00_0}k_{11_0}| \quad (49)$$

[7] showed that a general  $W$ -class state could be expressed as

$$(\alpha|100\rangle + \beta|010\rangle + \gamma|001\rangle + \delta|000\rangle)_{ABC} \quad (50)$$

where  $\{\alpha, \beta, \gamma, \delta\} \in \mathbb{R}$  and  $\alpha, \beta, \gamma > 0$ ,  $\delta \geq 0$ . We will without loss of generality take  $\gamma \geq \beta \geq \alpha$ .

We find for the state (50) that

$$S(\rho_A) = H_2(\lambda), \text{ where} \quad (51)$$

$$\lambda^2 - \lambda + \alpha^2(\beta^2 + \gamma^2) = 0 \quad (52)$$

Using (27), we find the corresponding concurrences

$$q(\rho_A) = 2\alpha\sqrt{\beta^2 + \gamma^2} \quad (53)$$

$$q(\rho_B) = 2\beta\sqrt{\alpha^2 + \gamma^2} \quad (54)$$

$$q(\rho_C) = 2\gamma\sqrt{\alpha^2 + \beta^2} \quad (55)$$

It is straightforward to see that  $q(\rho_C) \geq q(\rho_B) \geq q(\rho_A)$  and thus

$$E_{sp}^\infty(\psi_W) = S(\rho_B). \quad (56)$$

## B. A random distillation for $W$ -class states

We will see that a higher entanglement than the above may be obtained for a  $W$ -class state by first symmetrising it and then performing random distillation via the  $W$  protocol. Starting with the state (50) Alice applies the unitary

$$|0\rangle \longrightarrow \frac{\alpha}{\gamma}|0\rangle + \sqrt{1 - \left(\frac{\alpha}{\gamma}\right)^2}|2\rangle, \quad |1\rangle \longrightarrow |1\rangle \quad (57)$$

producing the state

$$\begin{aligned} & \left( \alpha|100\rangle + \frac{\beta\alpha}{\gamma}|010\rangle + \alpha|001\rangle + \frac{\delta\alpha}{\gamma}|000\rangle \right)_{ABC} \\ & + \sqrt{1 - \left(\frac{\alpha}{\gamma}\right)^2} |2\rangle_A (\beta|10\rangle + \gamma|01\rangle + \delta|00\rangle)_{BC} \end{aligned} \quad (58)$$

Alice then projects using (31). If she receives outcome  $G$  (with probability  $1 - P_{AF}$ ) the protocol terminates, otherwise Bob then applies the unitary

$$|0\rangle \longrightarrow \frac{\beta}{\gamma}|0\rangle + \sqrt{1 - \left(\frac{\beta}{\gamma}\right)^2}|2\rangle, \quad |1\rangle \longrightarrow |1\rangle \quad (59)$$

producing the state

$$\begin{aligned} & \frac{1}{\sqrt{P_{AF}}} \left[ \left( \frac{\alpha\beta}{\gamma}(|100\rangle + |010\rangle + |001\rangle) + \frac{\delta\alpha\beta}{\gamma^2}|000\rangle \right)_{ABC} \right. \\ & \left. + \sqrt{1 - \left(\frac{\beta}{\gamma}\right)^2} |2\rangle_B \left( \alpha|10\rangle + \alpha|01\rangle + \frac{\delta\alpha}{\gamma}|00\rangle \right)_{AC} \right] \end{aligned} \quad (60)$$

Bob likewise then projects using (31), the protocol terminating if he gets outcome  $G$ . If he gets outcome  $F$  (conditional probability  $P_{BF}$ ), the state obtained is

$$\frac{1}{\sqrt{P_{AF}P_{BF}}} \frac{\alpha\beta}{\gamma} \left( |100\rangle + |010\rangle + |001\rangle + \frac{\delta}{\gamma}|000\rangle \right)_{ABC} \quad (62)$$

which is a symmetric state on which the three parties perform the  $W$  protocol.

Thus for the overall protocol

$$\begin{aligned} q_{rnd}(\psi_W) & \geq (1 - P_{AF}) \times 2 \frac{\left(1 - \left(\frac{\alpha}{\gamma}\right)^2\right) \beta\gamma}{1 - P_{AF}} \\ & + P_{AF}(1 - P_{BF}) \times 2 \frac{\left(1 - \left(\frac{\alpha}{\beta}\right)^2\right) \alpha^2}{P_{AF}(1 - P_{BF})} \\ & + P_{AF}P_{BF} \times 3 \frac{\left(\frac{\alpha\beta}{\gamma}\right)^2}{P_{AF}P_{BF}} \\ & = 2 \left(1 - \frac{\alpha^2}{\gamma^2}\right) \beta\gamma + 2\alpha^2 + \frac{\alpha^2\beta^2}{\gamma^2} \end{aligned} \quad (63)$$

We use the Lemma

**Lemma 2:**

$$q_{rnd}(\psi_W) = 2 \left( 1 - \frac{\alpha^2}{\gamma^2} \right) \beta \gamma + 2\alpha^2 + \frac{\alpha^2 \beta^2}{\gamma^2} > q(\rho_B) = 2\beta \sqrt{\alpha^2 + \gamma^2} \quad (64)$$

**Proof:** See Appendix A.

Hence from (29)

$$E_{rnd}(\psi_W) \geq f(q_{rnd}(\psi_W)) > f(q(\rho_B)) = E_{sp}(\psi_W). \quad \square \quad (65)$$

### C. GHZ-class states

As noted in [1], the above inequality ( $E_{rnd}(\psi) > E_{sp}(\psi)$ ) is not generally true for GHZ class states, with the GHZ state itself, and more generally states of the form  $\alpha|000\rangle + \beta|111\rangle$  (for which  $E_{sp} = E_{rnd}$ ) providing a counterexample. One might wonder whether random distillation gives no advantage for any state in the GHZ class. Here, we answer this question in the negative. More specifically, we find an explicit example of a GHZ class state for which random distillation gives an advantage over distillation to predetermined parties.

Our example state is

$$|\psi_G\rangle = \alpha(|100\rangle + |010\rangle + |001\rangle) + \epsilon|111\rangle, \quad \epsilon = \sqrt{1 - 3\alpha^2}. \quad (66)$$

for  $0 < \{\alpha, \beta, \gamma, \delta, \epsilon\} \in \mathbb{R}$ . The three-tangle  $\tau_{ABC}$  [17] for this state is equal to  $16\epsilon\alpha^3$ , and being non-zero the state is thus [7] GHZ-class.

By symmetry of  $\psi_G$ , we have  $E_{sp}(\psi_G) = H_2(\alpha^2 + \epsilon^2)$ , and

$$f^{-1}(E_{sp}(\psi_G)) = \sqrt{8\alpha^2(1 - 2\alpha^2)} \quad (67)$$

From its symmetry and the analysis of section III A,  $\psi_G$  can be randomly distilled to obtain

$$q_{rnd} = 3\alpha^2. \quad (68)$$

It follows that  $q_{rnd}(\psi_G) > f^{-1}(E_{sp}(\psi_G))$  and hence  $E_{rnd}(\psi_G) > E_{sp}(\psi_G)$  for  $\alpha^2 > 8/25$ . I.e. there exist GHZ class states for which random distillation is advantageous and (as shown in [1]) others for which it is not.

## IV. SYMMETRIC DICKE STATES

While we do not have a general treatment of random distillation applied to pure states shared between  $> 3$  parties, it is clear that there are such states from which final states shared between fewer parties can be reliably obtained iff those parties are not predetermined. In [1] we gave the example of the  $M$ -party  $W$  state, (a symmetric

superposition of the  $M$ -qubit states with a single excited qubit)

$$|W_M\rangle = \frac{1}{\sqrt{M}}(|0\dots 01\rangle + |0\dots 010\rangle + (\text{permutations})) \quad (69)$$

to which applying the  $W$  protocol produces a randomly-shared  $W_{M-1}$  state. Considering a bipartite split of the initial and final states between one of the parties  $P$  who shares the final state and all other parties, we see that

$$S(\sigma_{Pf}) = H_2\left(\frac{1}{M-1}\right) > S(\sigma_{Pi}) = H_2\left(\frac{1}{M}\right) \quad (70)$$

where  $i$  and  $f$  denote initial and final states. Thus such a distillation cannot be reliably performed for predetermined final parties.

We can also consider a more general class of states whose entanglement properties are of some interest [18, 19, 20] - the  $M$ -party symmetric Dicke states [21, 22]. These are of the form

$$|\psi(M, N)\rangle = \frac{1}{\sqrt{{}^M C_N}} \sum |N \text{ 1s}, (M-N) \text{ 0s}\rangle \quad (71)$$

where  ${}^M C_N$  are the binomial coefficients

$${}^M C_N \equiv \frac{M!}{N!(M-N)!} \quad (72)$$

and the sum is over all permutations of the individual qubits. E.g.

$$|\psi(4, 2)\rangle = \frac{1}{\sqrt{6}}(|0011\rangle + |0110\rangle + |1100\rangle + |1001\rangle + |0101\rangle + |1010\rangle). \quad (73)$$

Considering the Von Neumann entropy of a party  $P$  we have

$$S(\sigma_P^{M,N}) = H_2\left(\frac{1}{{}^M C_N}\right) \quad (74)$$

and hence any LOCC distillation  $\psi(M, N) \rightarrow \psi(M', N')$  cannot be reliably performed for predetermined final parties if  ${}^{M'} C_{N'} < {}^M C_N$ .

However, we see that if we apply the  $W$  protocol to a state  $\psi(M, N)$  we can reliably obtain either a randomly-shared  $\psi(M-1, N)$  (applying the usual protocol) or  $\psi(M-1, N-1)$  (applying the  $W$  protocol but with  $|0\rangle$  and  $|1\rangle$  states reversed). Essentially the parties can reliably "drop" either a  $|0\rangle$  or  $|1\rangle$  from the terms of the state to produce a state randomly shared between one fewer party.

Given that the parties can also (by all applying a bit-flip operation) always reliably convert  $\psi(M, N) \rightarrow \psi(M, M-N)$ , we find that the parties can reliably perform

$$|\psi(M, N)\rangle \rightarrow |\psi(M', N')\rangle, \text{ or } |\psi(M', M' - N')\rangle \text{ if} \quad (75)$$

$$M' \leq M$$

$$N' \geq (M' - M) + N$$

many of which output states could not be achieved for predetermined final parties.

## V. RANDOM DISTILLATION IN THE MANY-PARTY LIMIT

In our previous paper [1], we show that random distillation is useful for the case of a single copy of the  $W$  state. One might wonder whether random distillation remains advantageous in the limit of many copies of a general pure state (including  $W$  states). Here we show that (according to our current definition) the answer is no.

In [1] we showed that one could randomly distill one EPR pair from a single  $W$  state compared to 0.92 EPRs per  $W$  between predetermined parties in the many-copy limit. Trivially, it follows that for multiple copies of the  $W$  state we can obtain advantageous random distillation in the context of  $E_t > E_{sp}$  - that is, many copies of the  $W$  state can produce more EPR pairs *in total* (summing up those between all pairs of parties) than can be obtained between predetermined parties.

However, this does not tell us whether random distillation remains useful for many copies of a pure state in our redefined sense of  $E_{rnd} > E_{sp}$  - obtaining more entanglement between only two parties when the two are not predetermined.

In what follows, we will discuss the case of two copies of  $W$  states and note that we find an advantage for random distillation for this case. More concretely, we can easily devise a simple two-copy analogue to the  $W$  protocol, in which three parties sharing two  $W$  states each repeatedly perform the two-qubit unitary

$$|00\rangle \longrightarrow \sqrt{1 - \epsilon^2}|00\rangle + \epsilon|2\rangle \quad (76)$$

(with all other states ( $|01\rangle, |10\rangle, |11\rangle$ ) mapping to themselves) combined with a projection into either a  $|2\rangle$  state or the  $SU(2) \otimes SU(2)$  subspace. As with the general three-qubit state, in this case repeated rounds change the overall state. We find, by considering a four-qubit measure analogous to  $q$ , that

$$E_{rnd}(W^{\otimes 2}) \geq -2[\zeta \log_2 \zeta - (0.5 - \zeta) \log_2 (0.5 - \zeta)] \approx 1.843, \text{ where} \quad (77)$$

$$\zeta = \frac{1 - \sqrt{1 - (\frac{8}{9})^2}}{4} \quad (78)$$

Hence

$$E_{rnd}(W^{\otimes 2}) > E_{sp}^\infty(W^{\otimes 2}) = 2H_2\left(\frac{1}{3}\right) \approx 1.837. \quad (79)$$

Hence there is an advantage to random distillation of  $W^{\otimes 2}$ , but the proven advantage is very marginal. We see that this extending this protocol in a naïve manner to more copies (i.e performing a unitary  $|0\rangle^{\otimes N} \rightarrow$

$\sqrt{1 - \epsilon^2}|0\rangle^{\otimes N} + \epsilon|2\rangle$  etc.) will not sustain the advantage, since for  $N$  copies the probability of success will fall roughly as  $O(\frac{1}{3^N})$ , while not predetermining the parties will at most triple the expected entanglement.

Confirming this idea more generally, we find in the limit of large  $N$ :

**Theorem 2:**

$$E_{rnd}(\psi^{\otimes N}) \longrightarrow E_{sp}(\psi^{\otimes N}), \quad N \rightarrow \infty. \quad (80)$$

In other words, as defined in (21) and (22),

$$E_{rnd}^\infty(\psi) = E_{sp}^\infty(\psi). \quad (81)$$

**Proof:**

This is shown by the result of [23], that for a LOCC protocol distilling EPR pairs from  $N$  copies of a two-party pure state  $\sigma_{AB}$ ,

$$|\sigma\rangle_{AB}^{\otimes N} \xrightarrow{\text{LOCC}} |\Phi\rangle_{AB}^{N'} \quad (82)$$

the probability of getting  $N' > NS(\rho_A)$  tends to 0 as  $N \rightarrow \infty$ . Specifically the probability shrinks as  $\exp(O(-N))$ . Note that this is stronger than the well-known result that optimally  $\langle N' \rangle = NS(\rho_A)$ , since it disallows improving on the optimum expected yield even some of the time.

Consider a process (16), where  $\psi = \phi_{A_1 \dots A_m}^{\otimes N}$ , for some pure state  $\phi$ . The optimum distillation to specified parties will be to some pair of parties  $A_I, A_J$ . where (from (9)) the distillation rate is  $S_\phi(A_I T_{IJ}^\phi)$  where  $S_\phi$  denotes Von Neumann entropy of the bracketed parties' reduced state of  $\phi$ ,  $T_{IJ}$  in general represents some group of parties not containing  $A_I$  or  $A_J$  and  $T_{ij}^\phi$  is the group that minimises  $S_\phi(A_i T_{ij})$ , i.e. for any fixed but arbitrary pair of parties  $A_i, A_j$ .

$$S_\phi(A_i T_{ij}^\phi) \leq S_\phi(A_i T_{ij}) \quad \forall \quad T_{ij}. \quad (83)$$

Thus, as  $N \rightarrow \infty$

$$E_{sp}(\psi) \longrightarrow NS_\phi(A_I T_{IJ}^\phi) \quad (84)$$

and

$$S_\phi(A_I T_{IJ}^\phi) \geq S_\phi(A_i T_{ij}^\phi) \quad \forall \quad ij \quad (85)$$

For  $E_{rnd}(\psi) > E_{sp}(\psi)$ , by the definition in (20) we require at least one possible output state  $\psi_f$  to have  $E_{sp}(\psi_f) > E_{sp}(\psi)$ . Let us consider one such  $\psi_f$ , denoted by  $\psi'_f$ , and occurring with some fixed probability  $p'_f$ . Suppose optimal distillation of  $\psi'_f$  (to specified parties) is to parties  $A_X$  and  $A_Y$  with the corresponding bipartite cut being between  $A_X T_{XY}^f$  on one side (using, here and below,  $f$  to denote quantities defined for reduced states of  $\psi'_f$ , analogously to  $\phi$  above) and its complementary set on

the other side. Similar to Eqs. (83) and (85), we have for each fixed but arbitrary pair  $i, j$ ,  $S_f(A_i T_{ij}^f) \leq S_f(A_i T_{ij})$  for all  $T_{ij}$  and  $S_f(A_X T_{XY}^f) \geq S_f(A_i T_{ij}^f)$  for all  $i, j$ . Then, in the many-copy limit

$$E_{sp}(\psi'_f) = S_f(A_X T_{XY}^f) > E_{sp}(\psi) = N S_\phi(A_I T_{IJ}^\phi) \quad (86)$$

However, from (83), (85) and (86) we have that

$$\begin{aligned} S_f(A_X T_{XY}^\phi) &\geq S_f(A_X T_{XY}^f) \\ &> N S_\phi(A_I T_{IJ}^\phi) \geq N S_\phi(A_X T_{XY}^\phi) \end{aligned} \quad (87)$$

Consider now a bipartite division of  $\psi$  between the group  $A_X T_{XY}^\phi$  acting as a single party (i.e. we allow joint quantum operations within this group) denoted by  $A$  and the group of all other parties acting as a single party  $B$ .  $A$  and  $B$  perform the above LOCC protocol independently on  $M$  copies of  $\psi$ . Then with probability  $(p_{f'})^M$ , they obtain  $M$  copies of  $\psi'_f$ . In the limit of large  $M$ , the parties  $A$  and  $B$  can, through LOCC, distill these copies to  $M S_f(A) > M N S_\phi(A)$  EPR pairs.

Thus  $A$  and  $B$  would be distilling more than  $M N S_\phi(A)$  EPR pairs from  $M N$  copies of  $\phi$ , and from [23] their success probability must be  $\exp(O(-M N))$ , hence  $p_{f'} \sim \exp(O(-N))$ . But for  $E_{rnd}(\psi) > E_{sp}(\psi)$  under these circumstances would require  $S_f(A_X T_{XY}^f) \sim \exp(O(N))$ , which would require a forbidden increase in Schmidt number across a bipartite split between group  $A_X T_{XY}^f$  and all other parties.

Hence in the limit of large  $N$ , we cannot have advantageous random distillation of  $N$  copies of a pure state.  $\square$ .

## VI. CONCLUSION

We have generalised several of the results noted for specific cases in [1]. We have more carefully defined what constitutes “random” distillation so that any apparent advantage in terms of entanglement yield is specifically due to the final parties not being predetermined. The advantageous random distillation we previously noted for the  $W$  and similar states has been shown to apply to the general  $W$ -class of three-qubit states (and the GHZ class not to have a consistent property in this respect). We have shown that for the important class of symmetric Dicke states our  $W$  protocol can achieve conversions between states which are not achievable for predetermined final parties. Finally we have shown that

advantageous random distillation does not occur in the many-copy limit, and hence is a property specific to individual quantum states that cannot be considered in a regularised form, in contrast to many other entanglement properties.

Clearly we have still only dealt with a limited class of states and the extremal conditions of a single copy or the many-copy limit. Our quantitative approach does not readily generalise to all states - e.g. for random distillation to final states shared between more than two parties, the lack of a standard entanglement measure makes the choice of target state more arbitrary, and an “advantageous” random distillation is less defined by a measure than by the probability of achieving a given target state. However, as demonstrated with Dicke states above, two-party entanglement measures can be used to determine whether or not such states are achievable between predetermined parties.

For distillation to two-party entanglement from multiple copies of a state, an open question is how any advantage due to random distillation scales with the number of copies, since we now know such advantage vanishes in the many-copy limit.

As noted in [1], even when the target states are two-party and thus the final entanglement is reasonably well-defined, the full “structure” of the output of random distillation would be defined by a probability distribution over final entanglements for given pairs of parties, rather than a single number. For example, the  $W$  protocol for a  $W$  state shared between parties  $A, B, C$  reliably produces an EPR pair between one of the three pairs of parties  $AB, BC, AC$ , with each pairs having a probability of  $1/3$  of receiving the EPR. As shown in [1], EPRs can be reliably produced from some  $W$ -like states which are not symmetric, but in this case the probability of getting an EPR is not the same for each pair. An interesting open question is what the optimum such probability distribution (in terms of  $E_{rnd}$ ) is for a given state, and how this can be determined from the form of the state.

The authors acknowledge financial support from NSERC, CIFAR, the CRC program, CFI, OIT, PREA, MITACS, CIPI and QuantumWorks.

## VII. APPENDIX A

Proof of Lemma 2 can be done algebraically as follows



$$q_{rnd}^2 - q(\rho_B)^2 = 4 \left( 1 - 2\frac{\alpha^2}{\gamma^2} + \frac{\alpha^4}{\gamma^4} \right) \beta^2 \gamma^2 + 4\alpha^4 + \frac{\alpha^4 \beta^4}{\gamma^4} + 8\alpha^2 \beta \gamma \left( 1 - \frac{\alpha^2}{\gamma^2} \right) + 4\frac{\alpha^4 \beta^2}{\gamma^2} + 4\frac{\alpha^2 \beta^3}{\gamma} \left( 1 - \frac{\alpha^2}{\gamma^2} \right) - 4\beta^2(\alpha^2 + \gamma^2) \quad (88)$$

$$= \alpha^2 \left[ -12\beta^2 + 8\frac{\alpha^2 \beta^2}{\gamma^2} + 4\alpha^2 + \frac{\alpha^2 \beta^4}{\gamma^4} + 8\beta \gamma \left( 1 - \frac{\alpha^2}{\gamma^2} \right) + 4\frac{\beta^3}{\gamma} \left( 1 - \frac{\alpha^2}{\gamma^2} \right) \right] \quad (89)$$

$$= \alpha^2 \left[ \beta^2 \left( 8\frac{\gamma}{\beta} + 4\frac{\beta}{\gamma} - 12 \right) + \alpha^2 \left( 8\frac{\beta^2}{\gamma^2} + 4 + \frac{\beta^4}{\gamma^4} - 8\frac{\beta}{\gamma} - 4\frac{\beta^3}{\gamma^3} \right) \right] \quad (90)$$

$$= \alpha^2 \left[ 4\beta^2 \left( \frac{\gamma}{\beta} - 1 \right) \left( 2 - \frac{\beta}{\gamma} \right) + \alpha^2 \left( \left( \frac{\beta^2}{\gamma^2} - \frac{2\beta}{\gamma} \right)^2 + 4 \left( 1 - \frac{\beta}{\gamma} \right)^2 \right) \right] \quad (91)$$

There are thus 3 terms in the above. We recall that  $0 < \alpha \leq \beta \leq \gamma$ . The first term is clearly  $\geq 0$  since  $\gamma \geq \beta$ , and the other two terms are clearly  $\geq 0$  since they are squared. The first and third terms are both equal to 0 iff

$\beta = \gamma$ , but in that case the second term is  $> 0$ . Thus

$$q_{rnd} > q(\rho_B) \quad \square. \quad (92)$$

- 
- [1] B. Fortesque, H.-K. Lo, Phys. Rev. Lett., **98**, 260501 (2007)
  - [2] I. Devetak, A.W. Harrow, A. Winter, arXiv:quant-ph/0512015v1
  - [3] A. Abeyesinghe, I. Devetak, P. Hayden, A. Winter arXiv:quant-ph/0606225v1
  - [4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett., **70** 1895 (1993)
  - [5] C. H. Bennett and S.J. Wiesner, Phys. Rev. Lett., **69** 2881, 1992
  - [6] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys.Rev. A, **53**, 2046 (1996)
  - [7] W. Dür, G. Vidal, J. I. Cirac, Phys. Rev. A **62**, 062314 (2000)
  - [8] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde Phys. Rev. A **65**, 052112 (2002)
  - [9] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2000)
  - [10] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, A. Uhlmann, Proc. Quantum Computing and Quantum Communications: 1st NASA Intl. Conf., Palm Springs (1998), Springer LNCS 1509, pp. 247-257, Heidelberg, (1999)
  - [11] T. Laustsen, F. Verstraete and S.J. Van Enk, Quant. Inf. Comp., **3** No.1, 64 (2003)
  - [12] J. A. Smolin, F. Verstraete and A. Winter, Phys. Rev. A, **72**, 052317 (2005)
  - [13] M. Horodecki, J. Oppenheim and A. Winter, Nature **436**, 673 (2005)
  - [14] G. Gour, Phys. Rev. A, **72**, 042318 (2005)
  - [15] G. Gour, R. W. Spekkens, Phys. Rev. A, **73**, 062331 (2006)
  - [16] W. K. Wootters, Quant. Inf. Comp. **1**, 27 (2001)
  - [17] V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A **61** 052306 (2000)
  - [18] N. Kiesel, C. Schmid, G. Tóth, E. Solano, and H. Weinfurter, Phys. Rev. Lett. **98**, 063604 (2007)
  - [19] G. Tóth, J. Opt. Soc. Am. B **24**, 275 (2007)
  - [20] J. K. Stockton, J. M. Geremia, A. C. Doherty, H. Mabuchi, Phys. Rev. A **67**, 022112 (2003)
  - [21] R. H. Dicke, Phys. Rev. **03**, 99 (1954)
  - [22] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, CUP, Cambridge, UK (1997)
  - [23] H.-K. Lo and S. Popescu, Phys. Rev. A, **63**, 022301 (2001)